Air Live®

www.ovislink.com.tw

WL-5460AP v2

Wireless Access Point

User's Manual

Powered by OvisLink Corp.

FCC Certifications

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

All trademarks and brand names are the property of their respective proprietors.

Specifications are subject to change without prior notification.

Table of Content

Introduction **4**

FEATURES 5

PARTS NAMES AND FUNCTIONS 6

FACTORY DEFAULT SETTINGS 8

WL-5460AP v2 *8*

Hardware Connection **9**

Check the LEDs: *9*

About the Wireless Operation Modes **10**

ACCESS POINT MODE 11

CLIENT MODE (INFRASTRUCTURE) 12

CLIENT MODE (AD-HOC) 13

BRIDGE MODE 14

REPEATER MODE (WDS REPEATER / UNIVERSAL REPEATER) 15

WISP MODE (CLIENT ROUTER / WISP+UNIVERSAL REPEATER) 16

Configuration **17**

LOGIN 17

MODE 18

AP Mode setting *19*

Security 20

Advanced Settings *26*

Access Control *29*

Client Mode Settings *30*

Bridge Mode Settings *32*

Repeater Mode Settings *34*

WISP mode Setting *36*

STATUS 40

System *40*

Statistics *42*

Active Clients *42*

TCP/IP 43

OTHER 45

Upgrade Firmware *45*

Reboot *45*

Save/Reload Settings *45*

Password *47*

INTRODUCTION

WL-5460APv2 is world's most popular multi-function access point. It features an impressive total of 7 wireless multi-function modes that are not available in normal access point. In addition, the ACK timeout and RSSI feature makes it suitable for long distance application. From ordinary AP application to Hotspot and WISP usage, you will find the WL-5460AP is the device you want.

WL-5460APv2 is an IEEE802.11b/g compliant 11 Mbps & 54 Mbps Ethernet Wireless Access Point. The Wireless Access Point is equipped with two 10/100 M Auto-sensing Ethernet ports for connecting to LAN and also for cascading to next Wireless Access Point.

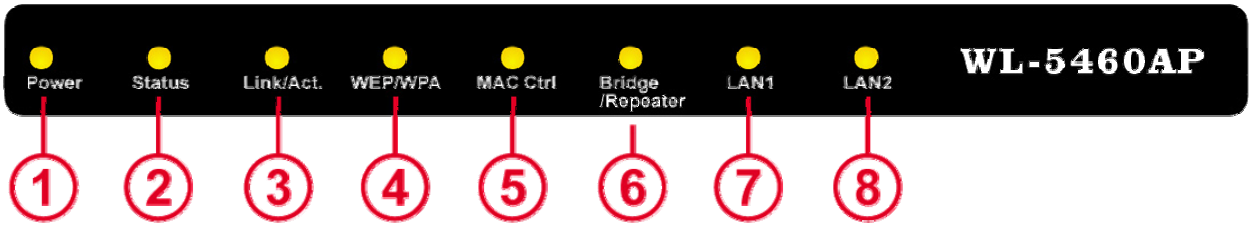
WL-5460APv2 provides 64/128bit WEP encryption, WPA and IEEE802.1x which ensures a high level of security to protect users' data and privacy. The MAC Address filter prevents the unauthorized MAC Addresses from accessing your Wireless LAN. Your network security is therefore double assured.
The web-based management utility is provided for easy configuration that your wireless network connection is ensured to be always solid and hassle free.

Features

1. 2x100Mbps LAN ports for Wireless AP cascade.,2MB flash,16MB SDRAM
2. 18dBm output Power
3. **AP** ,**Bridge**,**client** ,**WDS** Repeater, **Universal Repeater** mode.
4. **WISP Client Router**,**WISP+ Universal Repeater** mode
5. 802.1x WPA
6. Support data rate automatic fallback.
7. Automatic channel selection.
8. Client access control.
9. Support 802.1x/Radius client with EAP-TLS, TKIP, AES encryption.
10. Support IAPP.
11. Adjustable Tx power, Tx rate, and SSID broadcast.
12. ACK Timeout , Watch dog function.
13. Allow WEP 64/128 bit.
14. Web interface management.
15. Support System event log and statistics.
16. MAC filtering (For wireless only).

Parts Names and Functions

1. Front Panel: (LED Indicators) (5460AP / 5460AP v2)



	LED Indicator	Color	Status	
			Solid	**Flashing**
1	**Power**	Green	Turns solid green when power is applied to this device.	N/A.
2	**Status**	Red	Turns solid red when the device is booting, after boot successfully, the light turn off.	
3~6 Wireless	**Link/Act.**	Green	Turns solid green when connected and associated to at least a client station.	Receiving/ Sending data
	WEP/WPA	Orange	Turns solid orange when wireless security is enabled.	N/A
	MAC Ctrl	Orange	Turns solid orange when MAC Control is enabled.	N/A
	Bridge / Repeater	Orange	Turn solid **orange** when Bridge or Repeater is enabled.	N/A
7	**LAN 1**	Green	Turns solid green when linked to a local network.	Receiving/ Sending data
8	**LAN 2**			

Table 1: LED Indicators

2. Rear Panel: Connection Ports (5460AP / 5460AP v2)

	Port / button	Functions
A	12V DC	Connects the power adapter plug
B	LAN1	Connects to Ethernet
C	LAN2	Connects to Ethernet
D	(Factory) RESET	Press over 3 seconds to reboot this device. Press for over 10 seconds to restore factory settings. Performing the Factory Reset will erase all previously entered device settings.

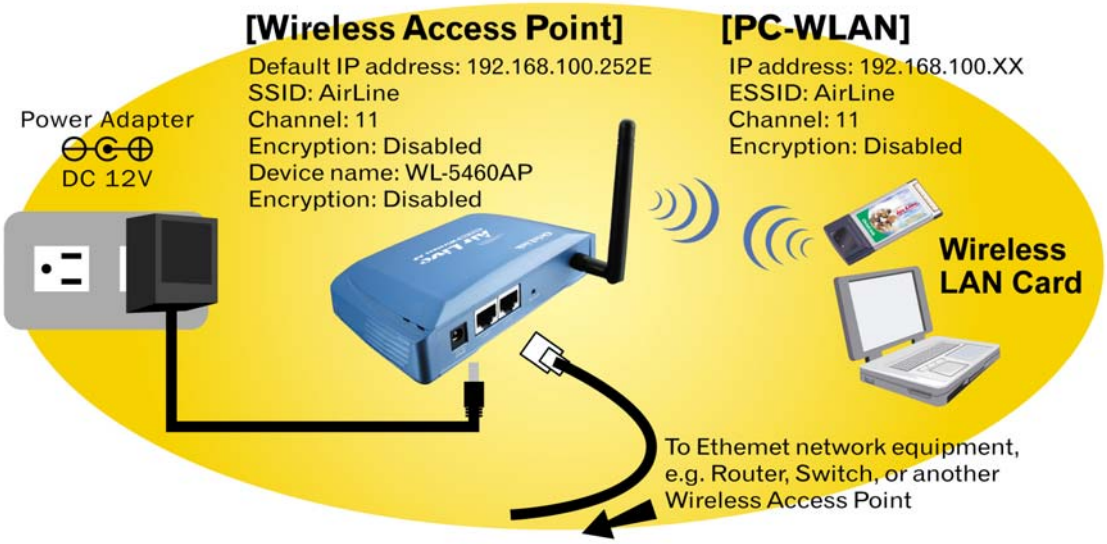
Table 2: Connection Ports

Factory Default Settings

Setting	Wireless Access Point
Device Name	**WL-5460AP v2**
SSID	Default value: **airlive**
Channel	**13**
WEP	Default value: **Disabled**
IP Address	**192.168.100. 252**
DHCP Server	• In **AP**, **Client**, and **Repeater** Mode, the default DHCP Server is **OFF** default . Please set your PC's IP to the same subnet as the AP to access the AP • In **WISP** mode, the DHCP server is turned **on**. Please restart your PC to renew the IP address.
DHCP Server IP Range	**192.168.100.100~192.168.100.200**

HARDWARE CONNECTION

Note: Before you starting hardware connection, you are advised to find an appropriate location to place the Access Point. Usually, the best place for the Access Point is at the center of your wireless network, with line of straight to all your wireless stations. Also, remember to adjust the antenna; usually the higher the antenna is placed, the better will be the performance.



1. **Connect to your local area network:** connect a **Ethernet cable** to one of the **Ethernet** port (LAN1 or LAN2) of this Wireless Access Point, and the other end to a hub, switch, router, or another wireless access point.

2. **Power on the device**: connect the included AC power adapter to the Wireless Access Point's power port and the other end to a wall outlet.

Check the LEDs:

The Power and ***LAN #*** LEDs should be ON. LAN# LED will even blink if there is traffic.

The ***Link/Act*** LED will be on in static when associated with a station and blink whenever this AP receives data packets in the air.

If the ***Status*** LED glows after self-test , it means this Wireless Access Point fails on self test. Please ask your dealer for technical support.

3. **Configure your PC:** Make sure your local PC(s) has wireless network adapter installed.

ABOUT THE WIRELESS OPERATION MODES

The WL-5460AP v2 device provides all 7 modes of wireless operational applications with :

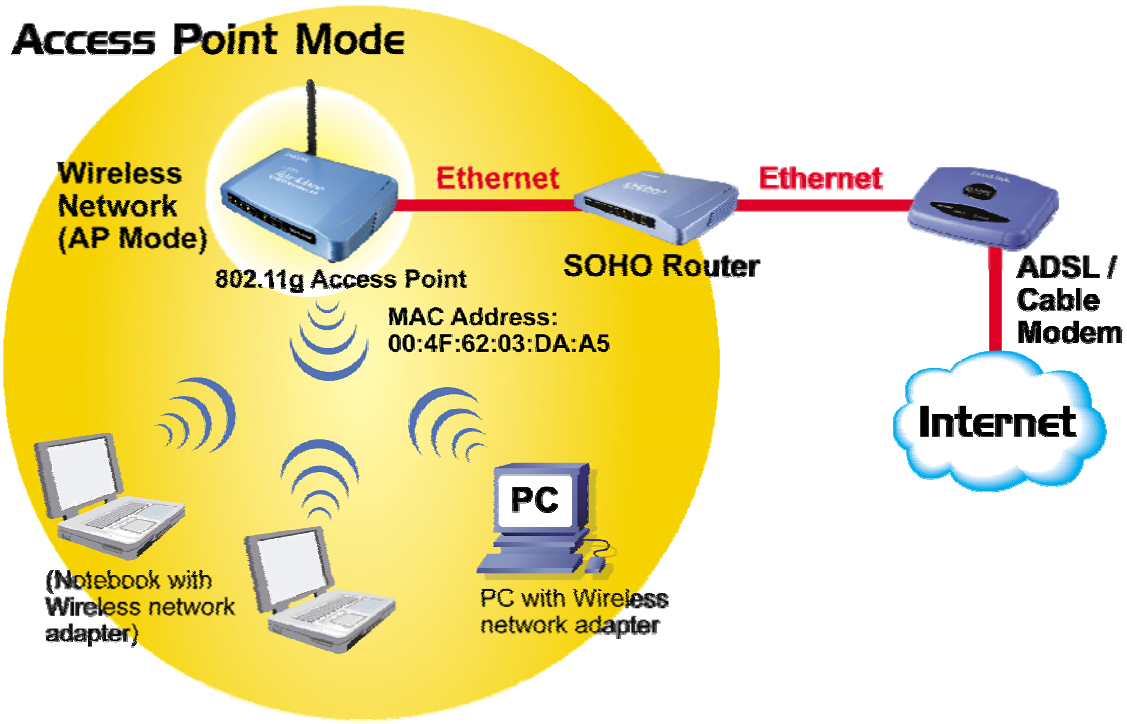
Access Point,
Bridge,
Client,
WDS Repeater,
Universal Repeater,
WISP (Client Router)
WISP + Universal Repeater

This device is shipped with configuration that is functional right out of the box. If you want to change the settings in order to perform more advanced configuration or even change the mode of operation, you can use the web-based utility provided by the manufacturer as described in the following sections.

Access Point Mode

When acting as an access point (default setting), this device connects all the stations (PC/notebook with wireless network adapter) to a wired network. All stations can have the Internet access if only the Access Point has the Internet connection. See the sample application below.

To set the operation mode to **Access Point,** please go to **"Mode →AP"** and click the **"Setup"** button.

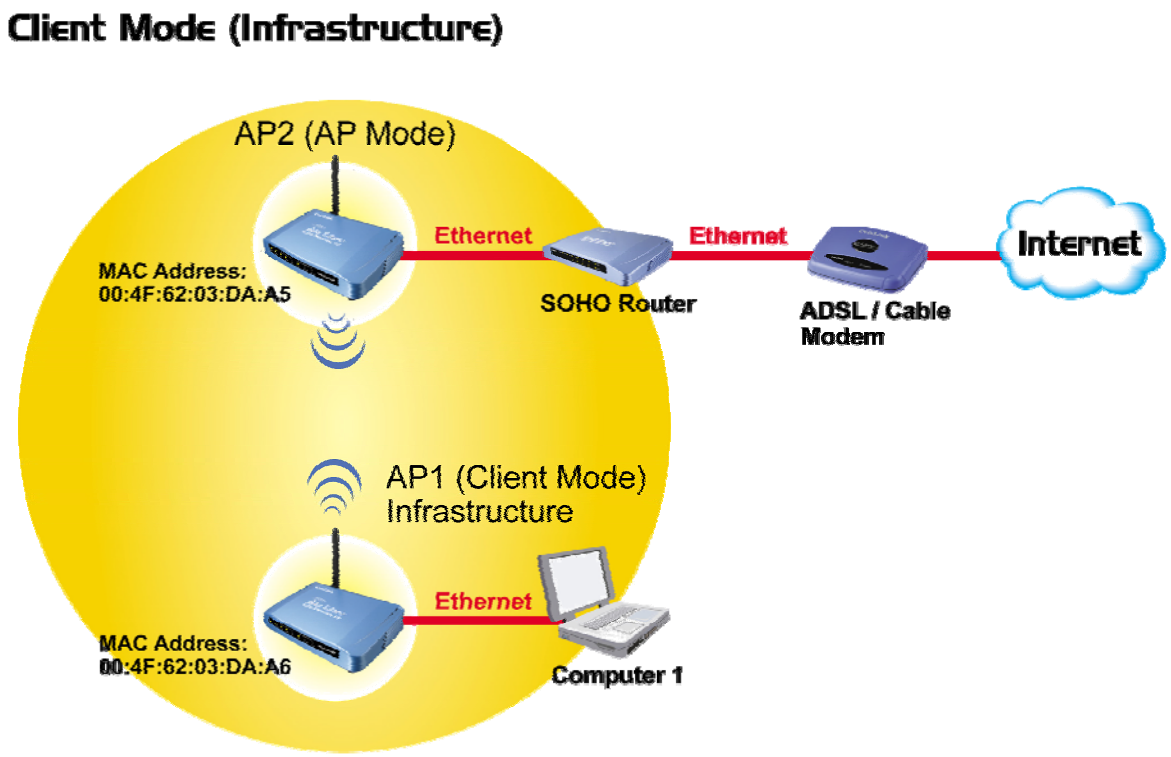


Client Mode (Infrastructure)

If set to Client (Infrastructure) mode, this device can work like a wireless station when it's connected to a computer so that the computer can send packets from wired end to wireless interface.

Refer to the illustration below. This station (AP1 plus the connected computer 1) can associate to another Access Point (AP2), and then can have the Internet access if the other Access Point (AP2) has the Internet connection.

To set the operation mode to **Client (Infrastructure),** please go to "**Mode →Client**", click the **"Setup"** button in the **"Network Type"** field, select as "**infrastructure"** for configuration

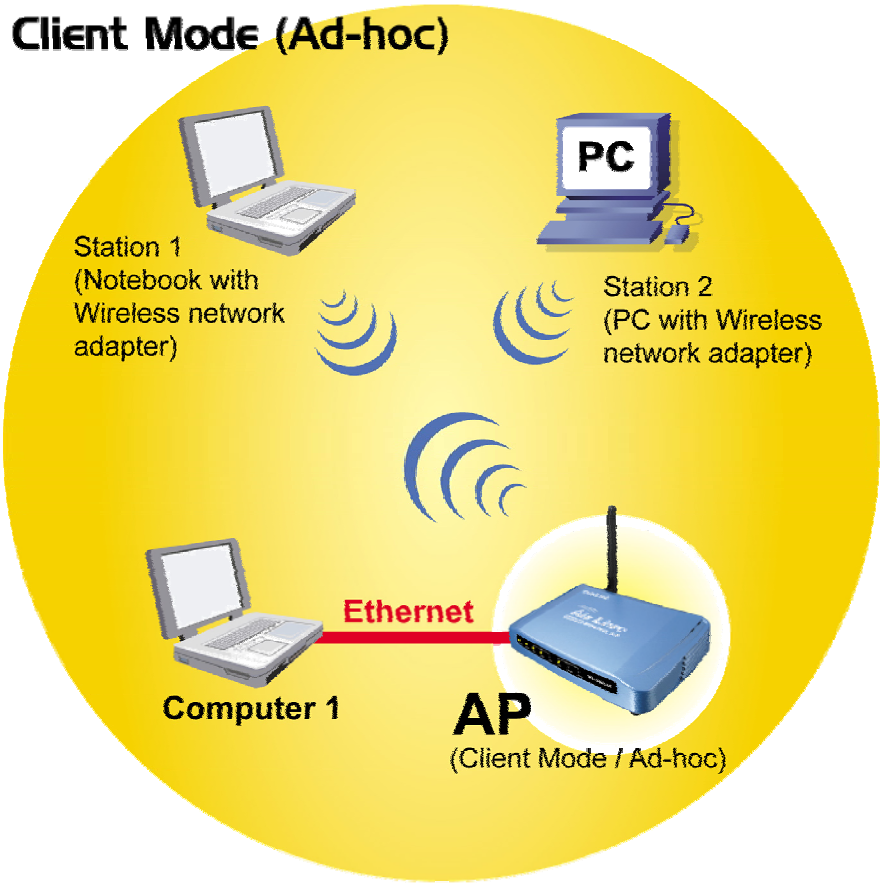


Client Mode (Ad-hoc)

If set to the Client (Ad-hoc) mode, this device can work like a wireless station when it is connected to a computer so that the computer can send packets from wired end to wireless interface. You can share files and printers between wireless stations (PC and laptop with wireless network adapter installed).

See the sample application below.

To set the operation mode to **Client (Ad-hoc),** please go to "**Mode →Client**", click the **"Setup"** button in the **"Network Type"** field, select as "**Ad-hoc"** for configuration



Bridge Mode

In this mode, 2 access points in two remote locations connect to each other to provide a wireless bridge between 2 remote LANs. It is mostly used by enterprise to connect 2 remote office's network together. The bridge modes are connected by using either the WDS (Wireless Distribution System) or Adhoc topology This feature is also useful when users want to bridge networks between buildings where it is impossible to deploy network cable connections between these buildings.

To set the operation mode to **Bridge,** please go to "**Mode →Brdige**", click the **"Setup"** button for configuration

Repeater mode (WDS Repeater / Universal Repeater)

WDS Repeater mode

A repeater's function is to extend the wireless coverage of another wireless AP or router.

For WDS repeater to work, the remote wireless AP/Router must also support WDS function.

To set the operation mode to **WDS Repeater,** please go to "**Mode →Repeater**", click the **"Setup"** button in the **"Network Type"** field, select as "**WDS Repeater "** for configuration

Universal Repeater mode

An universal repeater can also extend the wireless coverage of another wireless AP or router. But the universal repeater does not require the remote device to have WDS function. Therefore, it can work with almost any wireless device.

To set the operation mode to **WDS Repeater,** please go to "**Mode →Repeater**", click the **"Setup"** button in the **"Network Type"** field, select as "**Universal Repeater "** for configuration

Note: When you are using the universal repeater mode, please make sure the remote AP/Router 's WDS function is turned off..

WISP mode (Client Router / WISP+Universal Repeater)

WISP (Client Router) mode

In WISP mode, the AP will behave just the same as the Client mode for wireless function. However, router functions are added between the wireless WAN side and the Ethernet LAN side. Therefore, the WISP subscriber can share the WISP connection without the need for extra router.

To set the operation mode to **WISP mode,** please go to "**Mode →WISP**", click the **"Setup"** button for configuration

WISP + Universal Repeater mode

In this mode, the AP behaves virtually the same as the WISP mode, except one thing: the AP can also send wireless signal to the LAN side. That means the AP can connect with the remote WISP AP and the indoor wireless card, and then provide IP sharing capability all at the same time! However, the output power is divided between 2 wireless side and proper antenna installation can influence the performance greatly.

To set the operation mode to **WISP mode,** please go to "**Mode →WISP**", click the **"Setup"** button

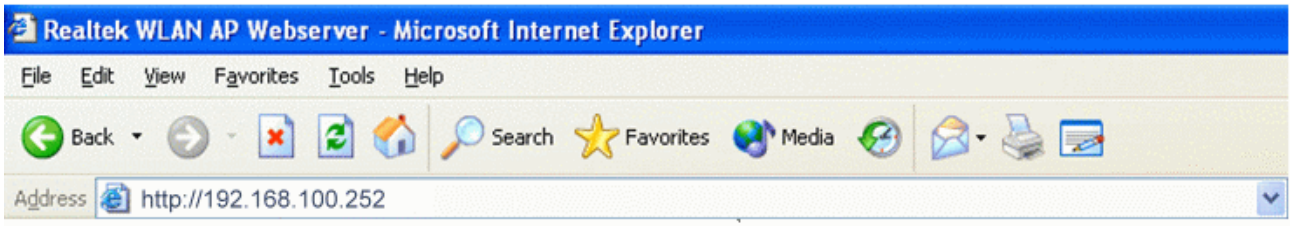
And select the **Enable Universal Repeater Mode check box** to enable this mode.

CONFIGURATION

Login

1. Start your computer. Connect an Ethernet cable between your computer and the Wireless Access Point.
2. Make sure your wired station is set to the same subnet as the Wireless Access Point, i.e. 192.168.100.252
3. Start your WEB browser. In the *Address* box, enter the following:

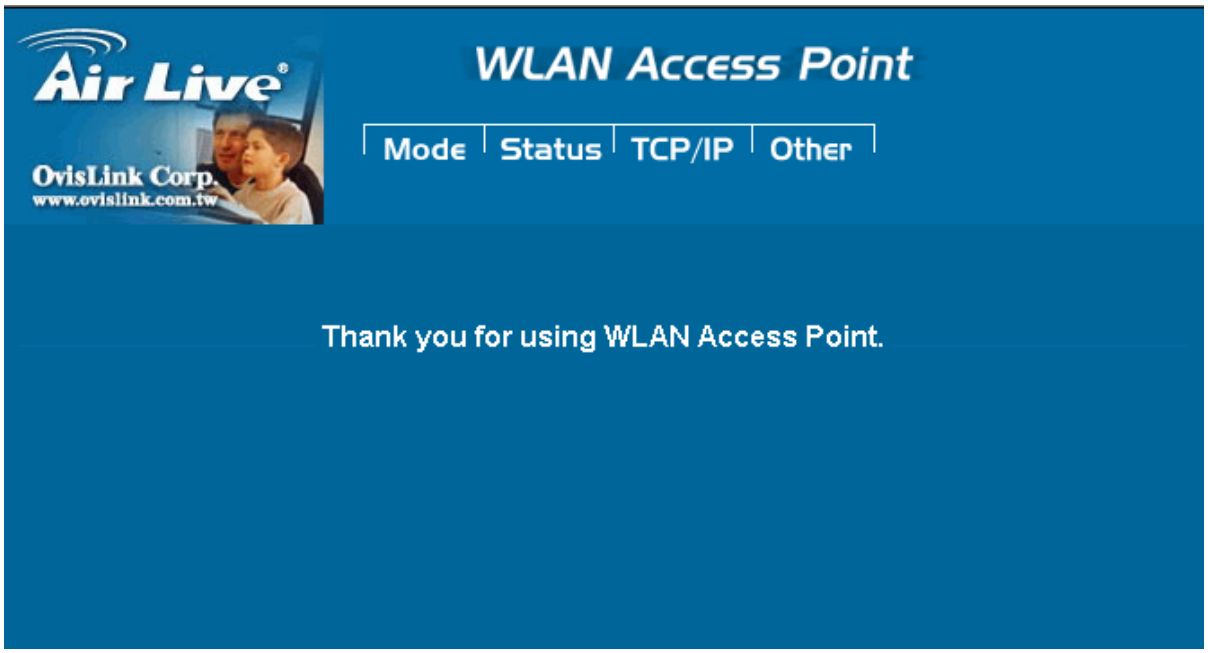
   http://192.168.100.252



The configuration menu is divided into four categories:

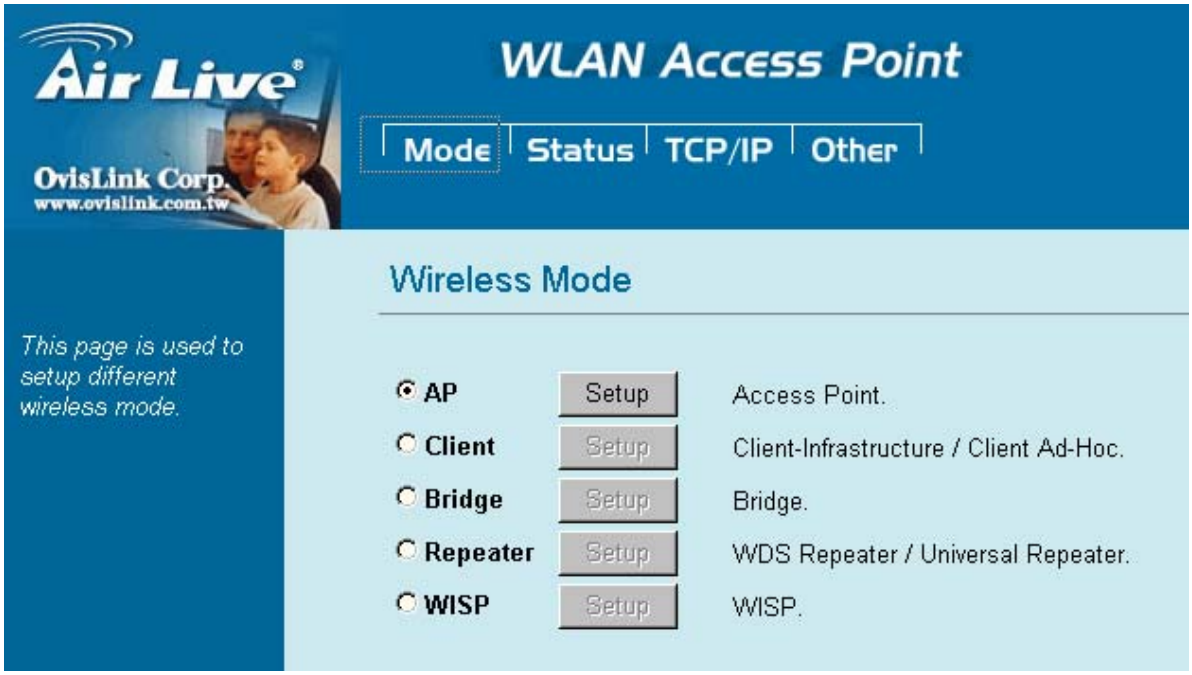
Mode, Status, TCP / IP, and **Other** .

Click on the desired setup item to expand the page in the main navigation page. The setup pages covered in this utility are described below.



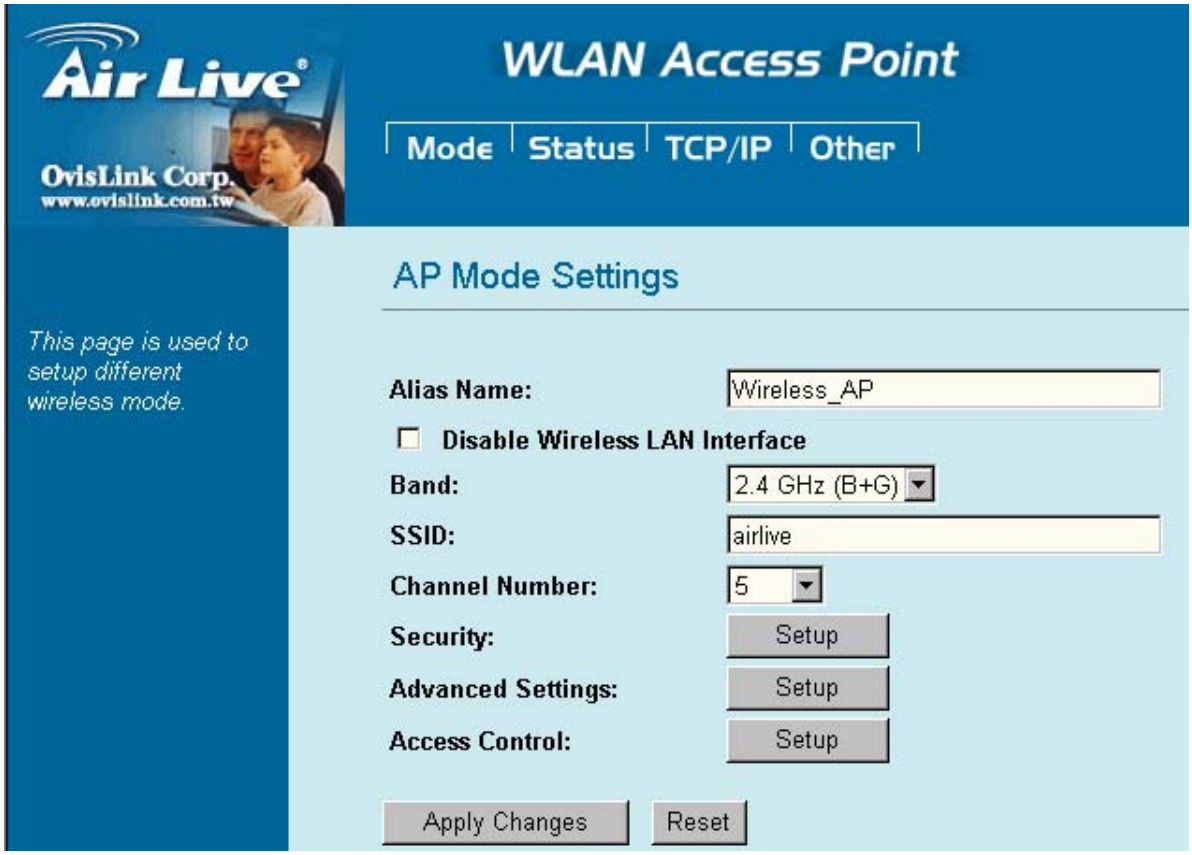
Mode

You can choose and setup different wireless mode and for detail configurations



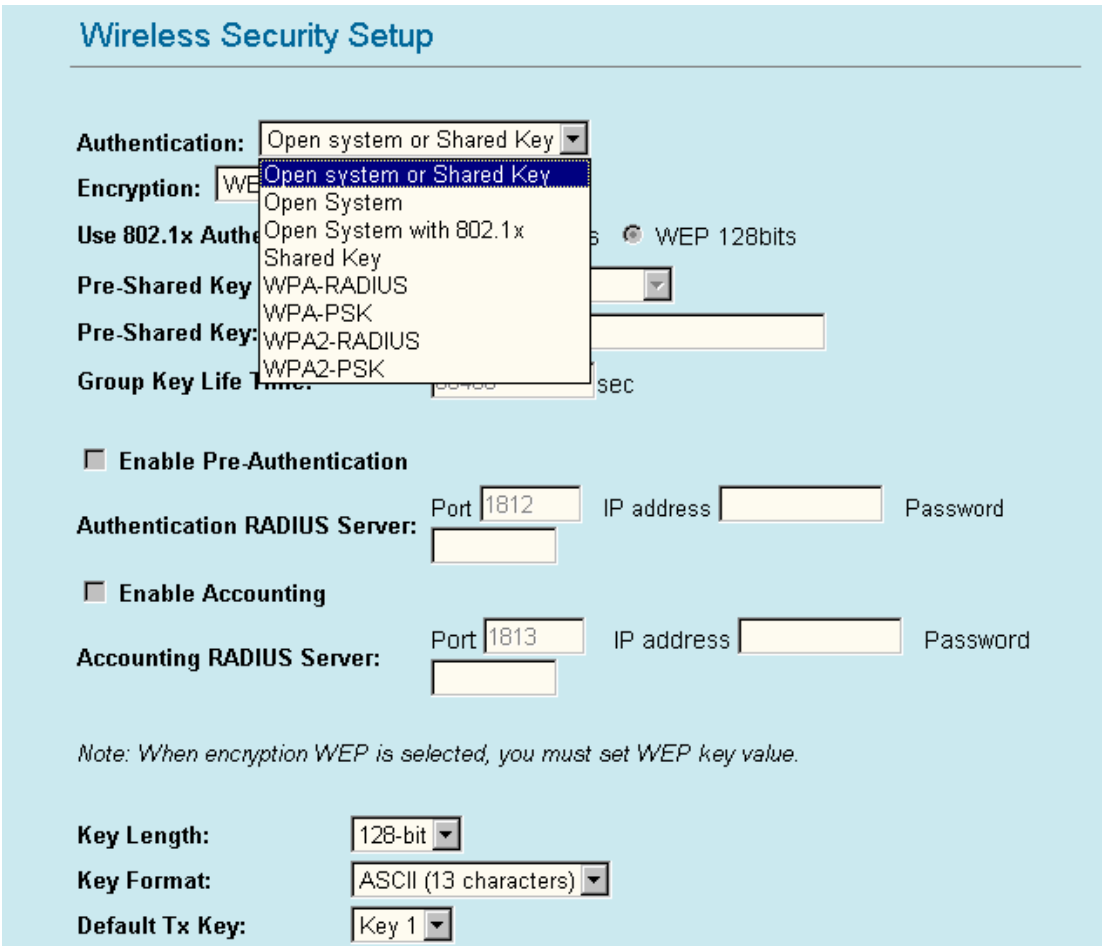
Wireless Mode	
AP	Select the AP and press Setup button for Wireless AP mode configuration
Client	Select the Client and press Setup button for Wireless Client mode configuration
Bridge	Select the Bridge and press Setup button for Wireless Bridge mode configuration
Repeater	Select the Repeater and press Setup button for WDS Repeater and Universal Repeater mode configuration
WISP	Select the WISP and press Setup button for WISP (Client Router) and WISP+ Universal Repeater configuration

AP Mode setting



Alias Name	You can set the alias name for this device. limited not exceed 32 characters
☐ **Disable Wireless LAN Interface**	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.

Channel Number	Allow user to set the channel **manually** or **automatically**. If set channel manually, just select the channel you want to specify. If "Auto" is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication. The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.
Security	Press the setup button for detail configurations



To provide a certain level of security, the IEEE 802.11 standard has defined two types of authentication methods: **Open System** or **Shared Key**. And WL-5460APv2 also support other wireless authentication and encryption methods for enhance your wireless network.

With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network and None data encryption. If you want secure your wireless network you need to setup wireless security related function to enable security network.

Security→ Authentication

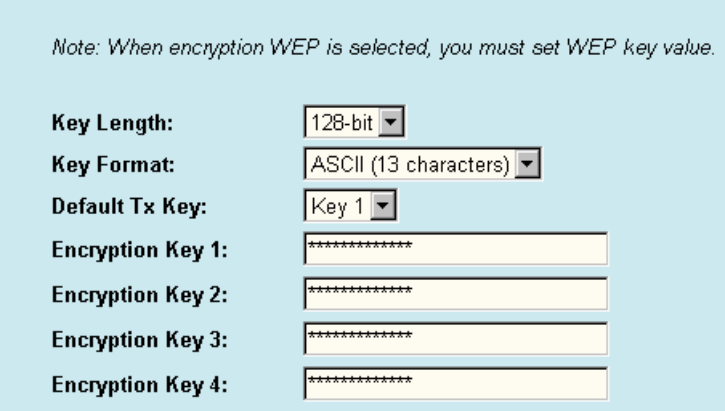
Open system or Shared Key.

Encryption**: None** (Encryption is set to **None** by default.**)**

If the Access Point is using **Open System**, then the wireless adapter will need to be set to the same authentication mode. **Shared Key** is used when both the sender and the recipient share a secret key. So you can choose Open system , or one Shared Key authentication method

Encryption: **WEP**

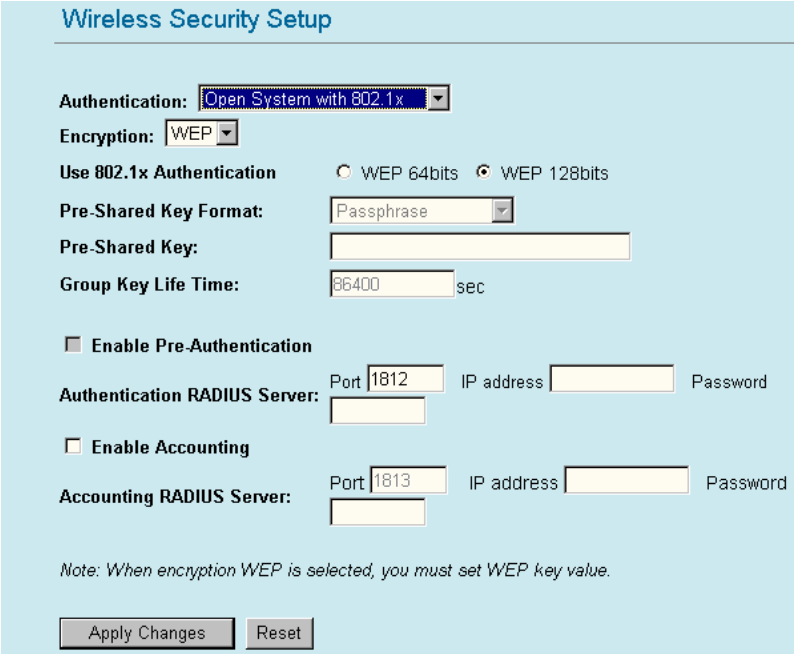
If selected, you must set WEP key value



- Key Length: to set **64bit** or **128bit** Encryption.
- Key format : Select **ASCII** if you are using ASCII characters (**case-sensitive**)Select **HEX** if you are using hexadecimal numbers (**0-9, or A-F**).
- Default Tx Key: you can enter 4 different Encryption Key and select one key to use as default.

Ten hexadecimal digits or **five ASCII characters** are needed if **64-bit WEP** is used; **26 hexadecimal digits** or **13 ASCII characters** are needed if **128-bit WEP** is used.

Open system with 802.1x



Encryption**:** **None**

No data encryption and **Use 802.1x Authentication** is disable.

Authentication RADIUS Server:

Enter the RADIUS Server IP address and Password provided by your ISP

Enable Accounting :

Enter the Accounting RADIUS Server IP address and Password provided by your ISP

Encryption: **WEP**

Use 802.1x Authentication is enabled and the RADIUS Server will proceed to check the 802.1x Authentication. and make the RADIUS server to issue the WEP key dynamically.

You can select WEP 64bits or WEP 128bits for data encryption)

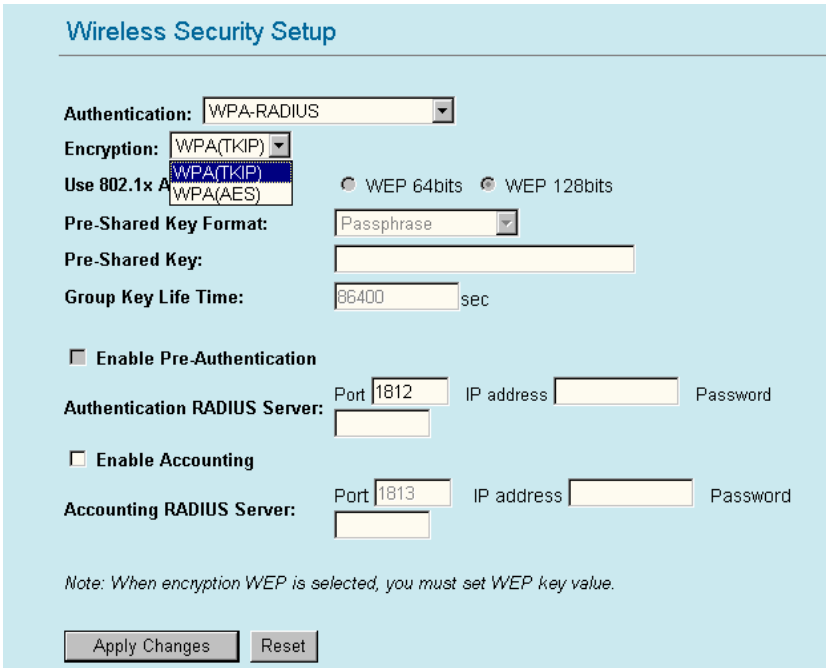
Authentication RADIUS Server:

Enter the RADIUS Server IP address and Password provided by your ISP

Enable Accounting :

Enter the Accounting RADIUS Server IP address and Password provided by your ISP

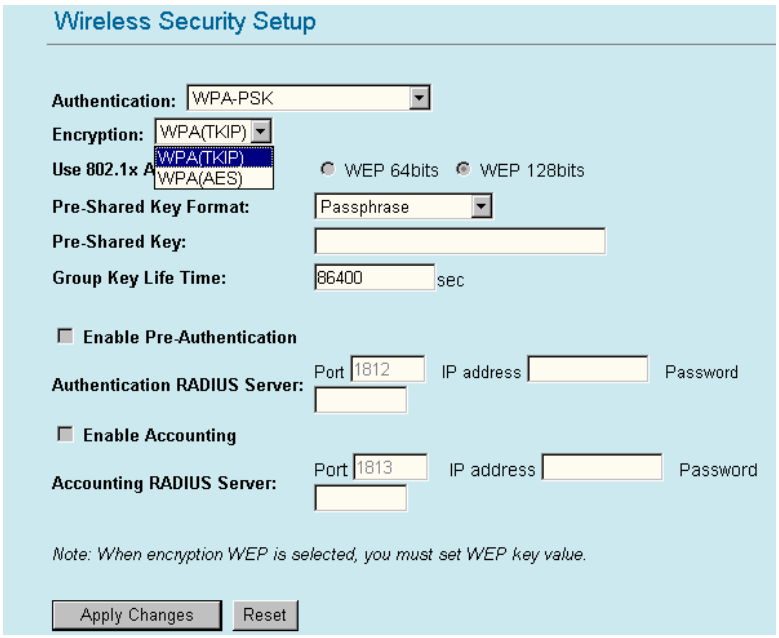
WPA-RADIUS



Encryption: **WPA(TKIP) / WPA(AES)**

WPA-RADIUS authentication use WPA (Wi-Fi Protect Access) data encryption for 802.1x authentication WPA is an encryption standard proposed by WiFi for advance protection by utilizing a password key (TKIP) or certificate. It is more secure than WEP encryption.

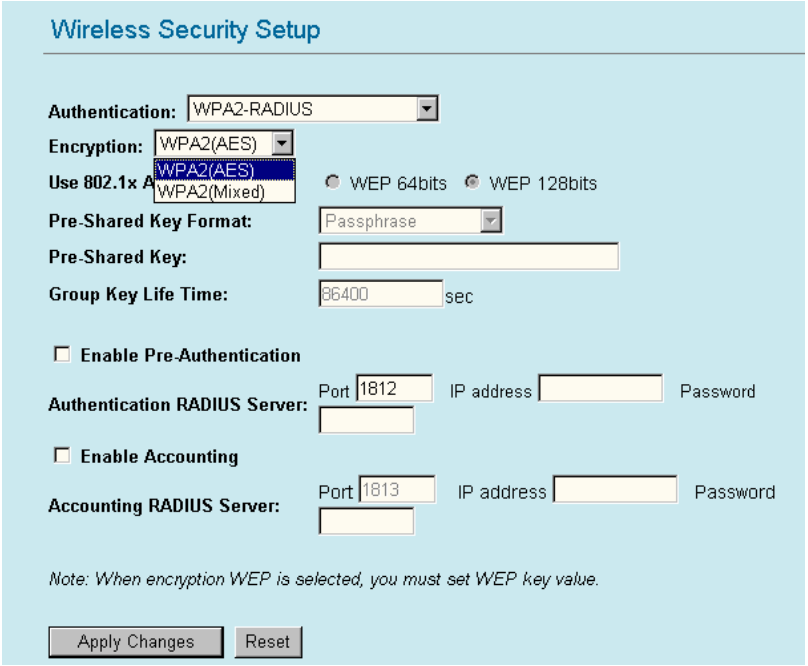
WPA-PSK



Wi-Fi Protected Access (WPA) with Pre-Shared Key (PSK) provides better security than WEP keys. It does not require a RADIUS server in order to provide association authentication, but you do have to enter a shared key for the authentication purpose. The encryption key is generated automatically and dynamically.

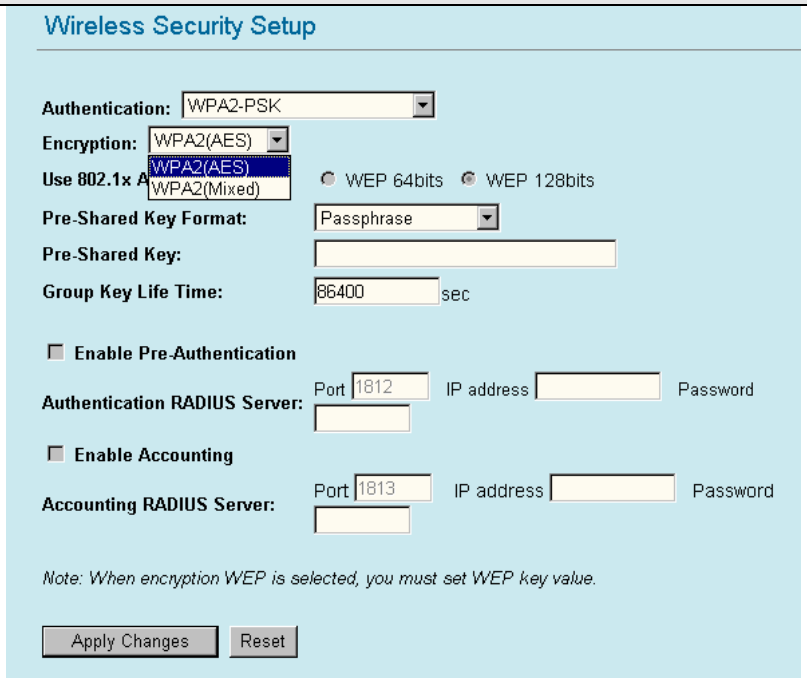
Use WPA-PSK authentication method, you can select WPA(TKIP) or WPA (AES) for data encryption

Pre-shared Key	Pre-Shared-Key serves as a password. Users may key in a 8 to 63 characters string to set the password or leave it blank, in which the 802.1x Authentication will be de-activated. Make sure the same password is used on client's end. There are two formats for choice to set the Pre-shared key, i.e. **Passphrase** and **Hex**. If **Hex** is selected, users will have to enter a 64 characters string. For easier configuration, the **Passphrase** (at least 8 characters) format is recommended.
Group Key Life Time	Enter the number of seconds that will elapse before the group key change automatically. The default is 86400 seconds.
WPA2-RADIUS	



Encryption	You can select WPA2(AES) or WPA2(Mixed) method for data encryption
Enable Pre-Authentication	The two most important features beyond WPA to become standardized through 802.11i/WPA2 are: pre-authentication, which enables secure fast roaming without noticeable signal latency. Pre-authentication provides a way to establish a PMK security association before a client associates. The advantage is that the client reduces the time that it's disconnected to the network.
Authentication RADIUS Server	**Port**: Enter the RADIUS Server's port number provided by your ISP. The default is **1812**. **IP Address:** Enter the RADIUS Server's IP Address provided by your ISP. **Password:** Enter the password that the AP shares with the RADIUS

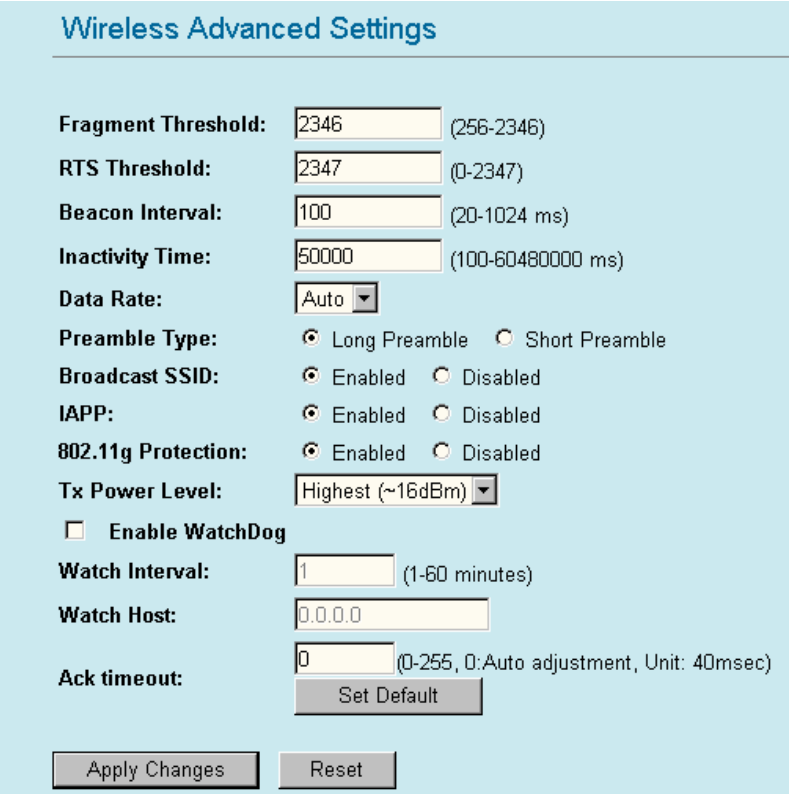
	Server.
WPA2-PSK	



WPA2-PSK authentication method is almost like WPA-PSK, you can choose the Pre-Shared Key format and enter the Pre-shared key , but use WPA2(AES) or WPA2(Mixed) for data encryption

Advanced Settings

It is not recommended that settings in this page to be changed unless advanced users want to change to meet their wireless environment for optimal performance



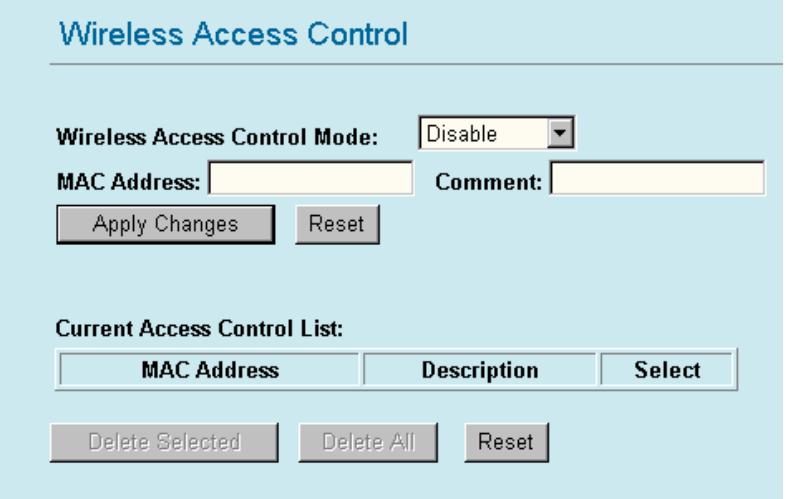
Fragment Threshold	Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If your 802.11g Wireless LAN PC Card often transmit large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. The default value is **2346**.
RTS Threshold	RTS Threshold is a mechanism implemented to prevent the "**Hidden Node**" problem. "Hidden Node" is a situation in which two stations are within range of the same Access Point, but are not within range of each other. Therefore, they are hidden nodes for each other. When a station starts data transmission with the Access Point, it might not notice that the other station is already using the wireless medium. When these two stations send data at the same time, they might collide when arriving simultaneously at the Access Point. The collision will most certainly result in a loss of messages for both stations. Thus, the RTS Threshold mechanism provides a solution to prevent data collisions. When you enable RTS Threshold on a

	suspect “hidden station”, this station and its Access Point will use a Request to Send (RTS). The station will send an RTS to the Access Point, informing that it is going to transmit the data. Upon receipt, the Access Point will respond with a CTS message to all station within its range to notify all other stations to defer transmission. It will also confirm the requestor station that the Access Point has reserved it for the time-frame of the requested transmission. If the “Hidden Node” problem is an issue, please specify the packet size. *The RTS mechanism will be activated if the data size exceeds the value you set.*. The default value is **2347**. **Warning:** Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy. This value should remain at its default setting of **2347**. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.
Beacon Interval	Beacon Interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Data Rate	By default, the unit adaptively selects the highest possible rate for transmission. Select the basic rates to be used among the following options: Auto, 1, 2, 5.5, 11or 54 Mbps. For most networks the default setting is **Auto** which is the best choice. When **Auto** is enabled the transmission rate will select the optimal rate. If obstacles or interference are present, the system will automatically fall back to a lower rate.
Preamble Type	A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a "noisy" network environment, the Preamble Type should be set to **Long Preamble**. The **Short Preamble** is intended for applications where minimum overhead and maximum performance is desired. If in a "noisy" network environment, the performance will be decreased.
Broadcast SSID	Select **enabled** to allow all the wireless stations to detect the SSID of this Access Point.

IAPP	IAPP (Inter Access Point Protocol) is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and a secure exchange of station's security context between current access point (AP) and new AP during handoff period.
802.11g Protection	The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operation. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network's performance.
TX Power Level	For countries that impose limit on WLAN output power, it might be necessary to reduce TX (transmit) power. The legal limit is measured as the output power at antenna end.. You can select TX Power Level for Highest 16dbm(default),High(15dbm),Middle(13dbm),Low(10dbm),Lowest(3dbm) Please check with your local authority about RF Power allowed in your country
Enable Watch dog	Check and enable this watch dog function
Watch Interval	Setup the interval time for watch dog function between 1 to 60 mins
Watch Host	Enter the watch dog host ip address .
ACK Timeout	When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. If the ACK is NOT received within that timeout period then the packet will be re-transmitted resulting in reduced throughput. If the ACK setting is too high then throughput will be lost due to waiting for the ACK Window to timeout on lost packets. By having the ability to adjust the ACK setting we can effectively optimize the throughput over long distance links. This is especially true for 802.11a and 802.11g networks You can set as default for auto adjustment.
Apply Change	Press to save the new settings on the screen.
Reset	Press to discard the data you have entered since last time you press Apply Change.

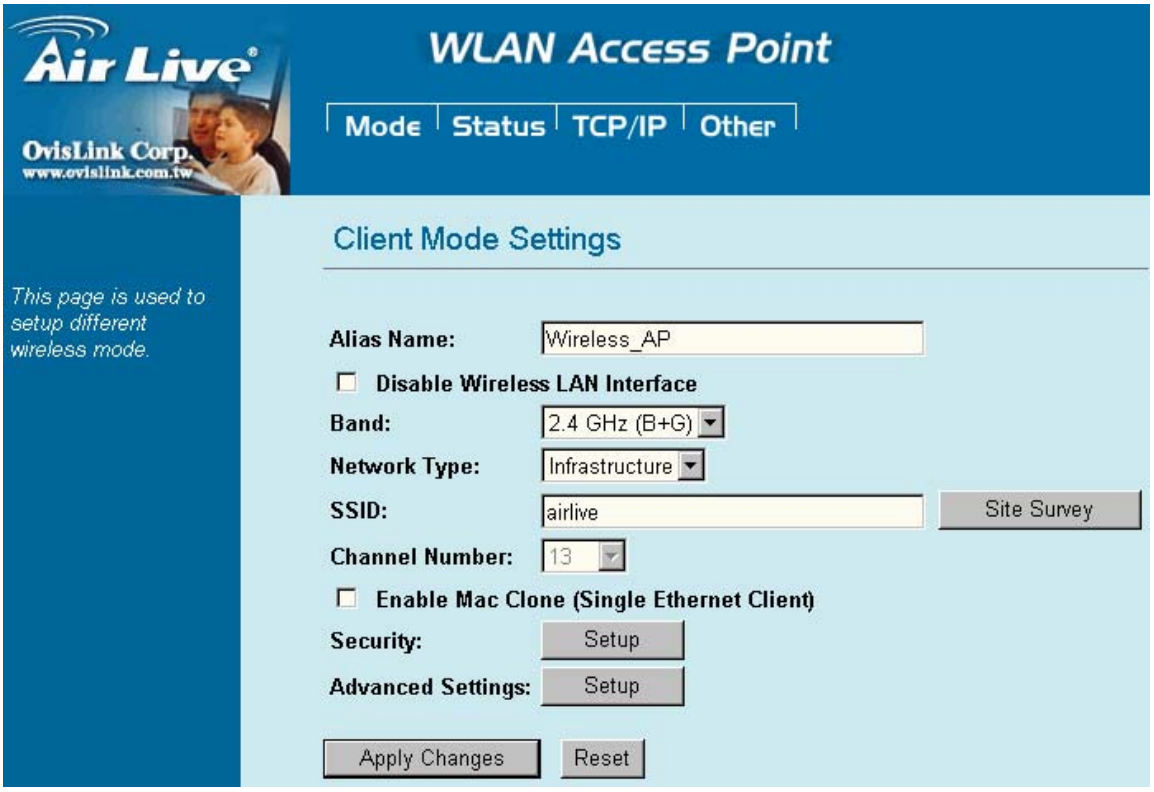
Access Control

When **Enable Wireless Access Control** is checked, only those clients whose wireless MAC addresses listed in the access control list can access this Access Point. If the list contains no entries with this function being enabled, then no clients will be able to access this Access Point.

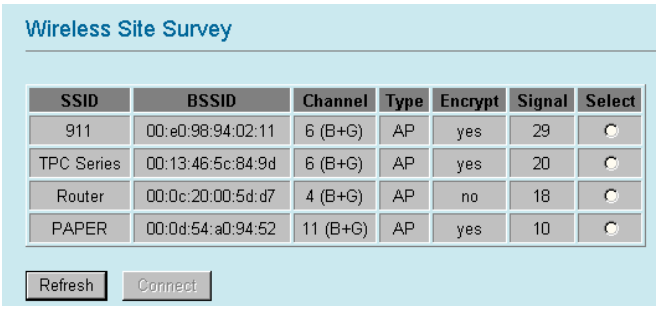


Wireless Access Control Mode	Select the Access Control Mode from the pull-down menu. **Disable**: Select to disable Wireless Access Control Mode. **Allow Listed**: Only the stations shown in the table can associate with the AP. **Deny Listed**: Stations shown in the table won't be able to associate with the AP.
MAC Address	Enter the MAC Address of a station that is allowed to access this Access Point.
Comment	You may enter up to 20 characters as a remark to the previous MAC Address.
Apply Changes	Press to save the new settings on the screen.
Reset	Press to discard the data you have entered since last time you press Apply Change.
Delete Selected	To delete clients from access to this Access Point, you may firstly check the **Select** checkbox next to the MAC address and Comments, and press **Delete Selected**.
Delete All	To delete all the clients from access to this Access Point, just press **Delete All** without selecting the checkbox.
Reset	If you have made any selection, press **Reset** will clear all the select mark.

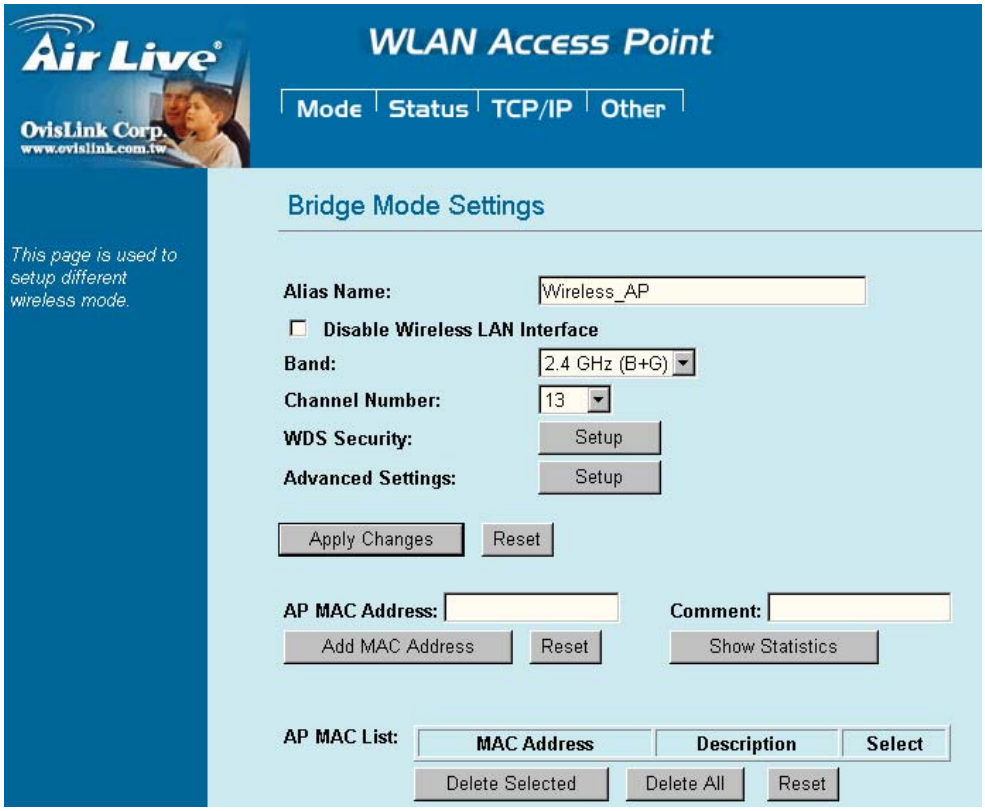
Client Mode Settings



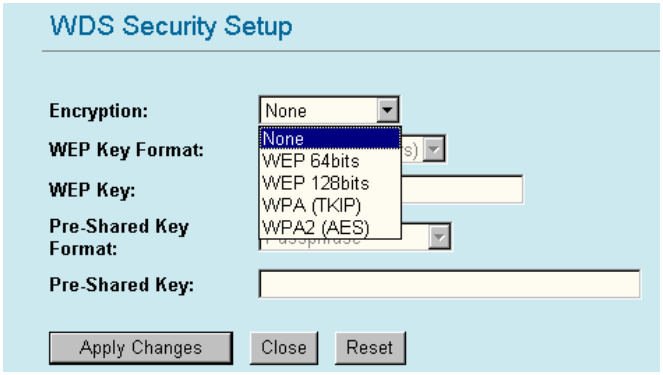
Alias Name	You can set the alias name for this device. limited not exceed 32 characters
☐ **Disable Wireless LAN Interface**	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
Network Type	Client mode have two Network type : **Infrastructure** A wireless network that is built around one or more access points, providing wireless clients access to wired LAN or Internet service. It is the most popular WLAN network structure today. **AdHoc** wireless network do not use wireless AP orrouter as the central hub of the network. Instead, wireless client are connected directly to each other.

SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.
Site Survey	 Site survey displays all the active Access Points and IBSS in the neighborhood. you can select one AP to associate. Press Site Survey button to search the wireless device that this client want to connect.
Channel Number	Allow user to set the channel **manually** or **automatically**. If set channel manually, just select the channel you want to specify. If "Auto" is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication.All stations communicating with the Access Point must use the same channel. when setup infrastructure of Client mode, the channel number can not Be changed. You have to go to AP mode to change the channel number
Enable MAC Clone	Check the box to enable MAC Clone for Single Ethernet Client
Security	Please refer the AP mode settings→ Security for details., in client mode are not supported with RADIUS 802.1x authentication.
Advance Setting	Please refer the AP mode settings→ Advance Setting for details.

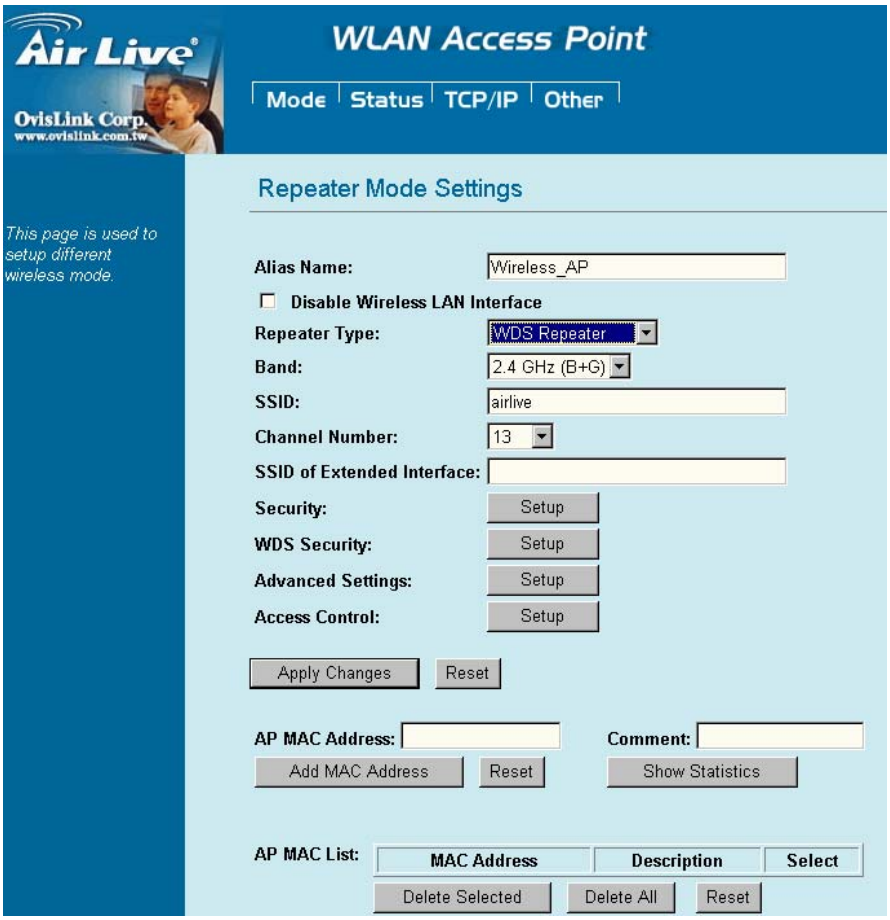
Bridge Mode Settings



Alias Name	You can set the alias name for this device. limited not exceed 32 characters
☐ **Disable Wireless LAN Interface**	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
Channel Number	In Bridge mode, both wireless AP/Router device need set to the same Channel number.

WDS Security	 To enable security between wireless AP/Router , you can select WEP(64bits),WEP(128bits),WPA (TKIP),WPA2(AES) for data encryption For WPA/WPA2 encryption, you need enter the Pre-Shared Key Information for the authentication purpose
Advance Setting	Please refer the AP mode settings→ Advance Setting for details.
AP MAC address	Enter 12 digits in hex numbers in the AP MAC address (**BSSID**) field and press the Add MAC Address Button to associate with other's Wireless access point. Before you want to use bridge mode to connect each other to provide A wireless bridge between 2 remote LANs, you need add the BSSID of other's wireless AP first.
Delete Selected	To delete bridge from access to this Access Point, you may firstly check the **Select** checkbox next to the MAC address and Comments, and press **Delete Selected**.
Delete All	To delete all the clients from access to this Access Point, just press **Delete All** without selecting the checkbox.
Security	Please refer the AP mode settings→ Security for details., but bridge mode are not supported with RADIUS 802.1x authentication.

Repeater Mode Settings



Alias Name	You can set the alias name for this device. limited not exceed 32 characters
☐ **Disable Wireless LAN Interface**	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Repeater Type	You can select two Repeater Type : **WDS Repeate**r/ **Universal Repeater.**
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be

	permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network
Channel Number	The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.
SSID of extended Interface	**When in Universal Repeater mode, you have to enter the ESSID of other's AP/Router that this device want to connect.** The device SSID and the SSID of extended interface can be the same or different. When you are using the universal repeater mode, please make sure the remote AP/Router WDS function is turned off.. **When use WDS Repeater mode, this field is no function**
Security	Please refer the AP mode settings→ Security for details., This setting is use between Wireless client and this device.
WDS Security	Please refer to the Bridge mode settings → WDS Security for details This setting is use between both wireless AP/Router device.
Advance Setting	Please refer the AP mode settings→ Advance Setting for details.
Access Control	Please refer to the Access Control chapter for details.
AP MAC address	Enter 12 digits in hex numbers in the AP MAC address (**BSSID**) field and press the Add MAC Address Button to associate with other's Wireless access point. Before you want to use WDS Repeater mode, you have to enter the other's AP/Router MAC address that the device want to connect. **When use Universal Repeater mode, this field is no function.**

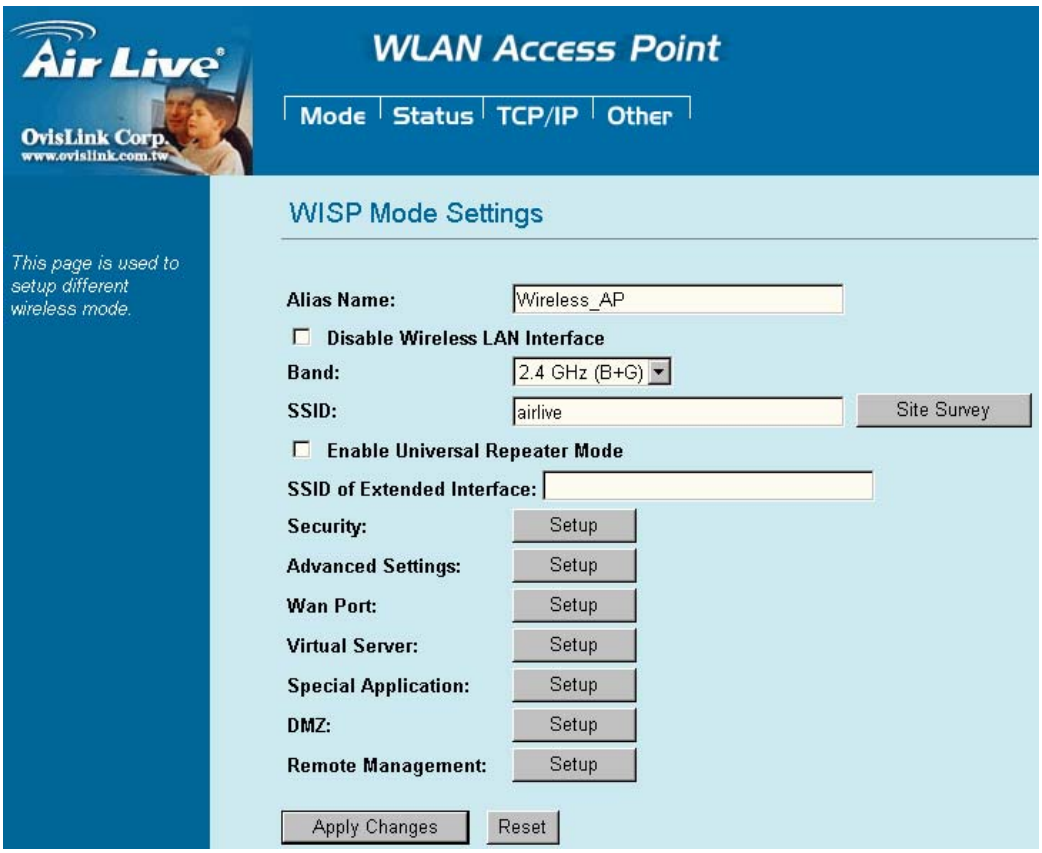
WDS Repeater mode:

1. both connected wireless AP/Router device have to set same channel number
2. enter other's AP/Router MAC address (BSSID)to add into AP MAC address list
3. apply changes to take effect

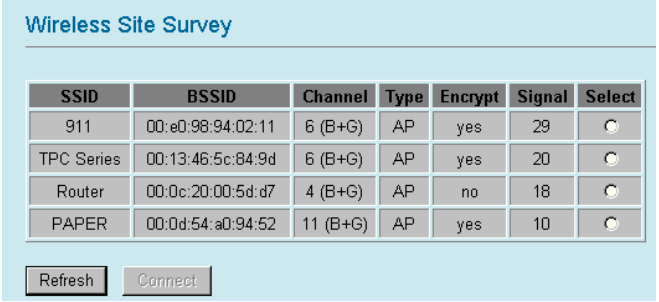
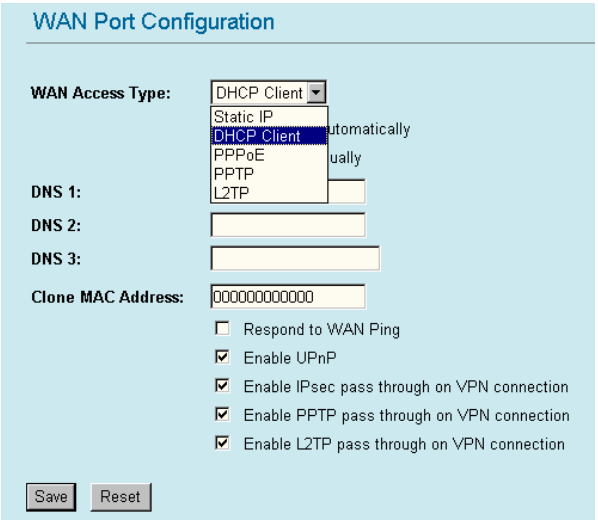
Universal Repeater mode:

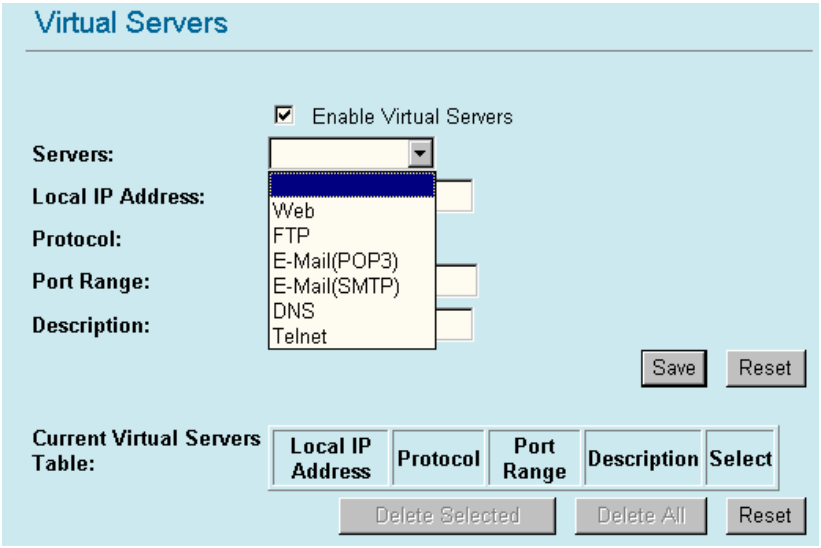
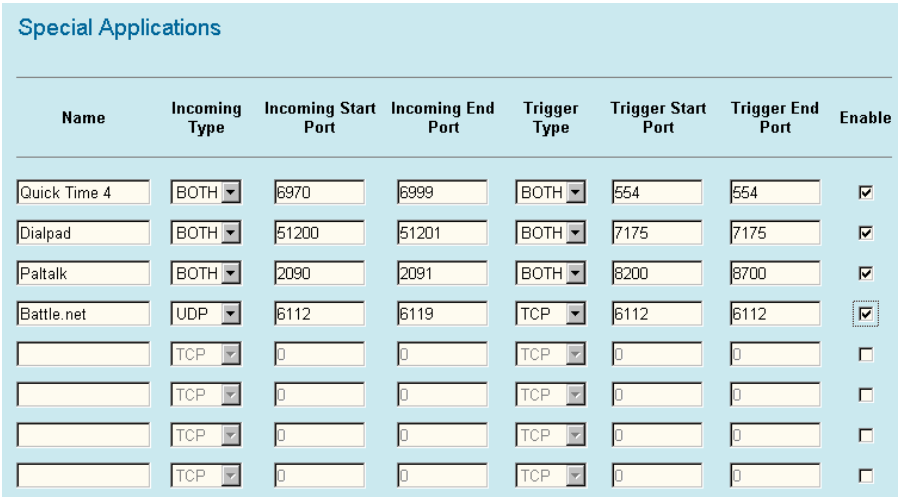
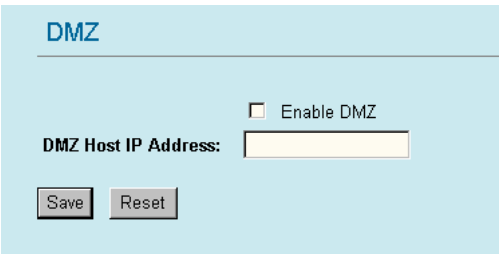
1. both connected wireless AP/Router device have to set same channel number
2. enter the other's AP/Router SSID(ESSID) to "SSID of extended interface" field (both AP/Router 's ESSID can be the same or different.)
3. apply changes to take effect.

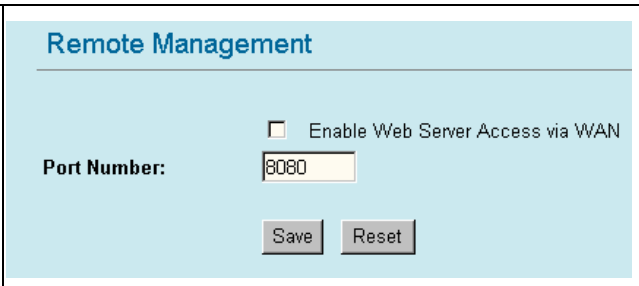
WISP mode Setting



Alias Name	You can set the alias name for this device. limited not exceed 32 characters
☐ **Disable Wireless LAN Interface**	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. In WISP mode, you have to enter the WISP Outdoor AP SSID manually or click the "site survey" button to connect and get SSID automatically.

Site Survey	 Site survey displays all the active Access Points and IBSS in the neighborhood. you can select one AP to associate. Press Site Survey button to search the wireless device that this client want to connect. In WISP mode, you have to select the WISP outdoor AP and connect.
☐ **Enable Universal Repeater**	Check this box will enable universal repeater function,that means this AP can connect to remote WISP AP and also can provide IP sharing Capability for Wireless LAN at same time.
SSID of extended Interface	When you check and enable the Universal Repeater, you have to enter SSID of other AP in this filed.
Security	Please refer the AP mode settings→ Security for details., This setting is use between Wireless client and this device. but not supported with RADIUS 802.1x authentication.
Advance Setting	Please refer the AP mode settings→ Advance Setting for details.
WAN port	 You can select many WAN Access Type : Static IP , DHCP Client, PPPOE, PPTP ,and L2TP for WAN connection depend on you WISP provided

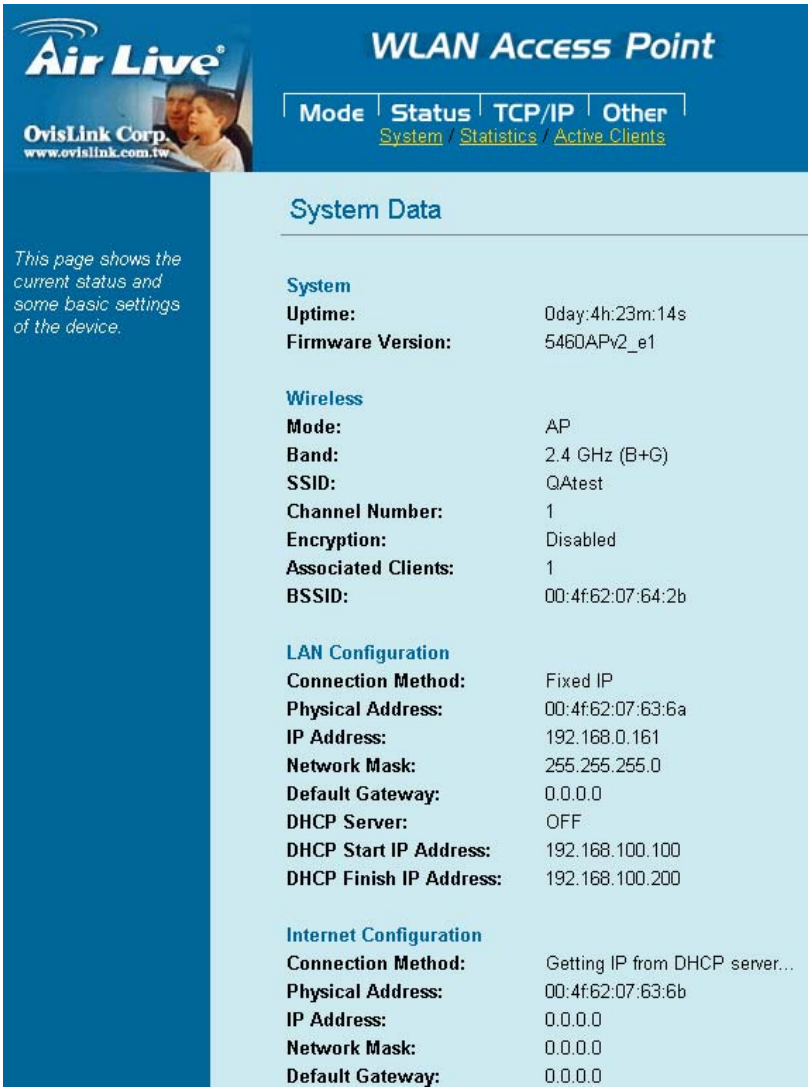
Virtual Server	 In WISP mode, you can setup and enable Virtual server function Like Web, FTP, Email, DNS, Telnet srever Select one virtual server type and enter the Local IP address, Local Port Range and click the save button.
Special Application	 You can enable some system default special application, like Qucktime 4 Audio/Video application, Dialpad internet phone service. or define the special application manually, select the incoming type (TCP/UDP) Incoming start ~ End port ,Trigger Start~End port. Select the Trigger Type.
DMZ	 Enable DMZ and enter the DMZ Host ip address.

Remote Management	 Enable the Web server that can be accessed via WAN.
Apply changes	After setup for this WISP mode, click the Apply Changes will take effect and act as WISP mode.

Status

In this screen, you can see the current settings and status of this Access Point. You can change settings by selecting specific tab described in below.

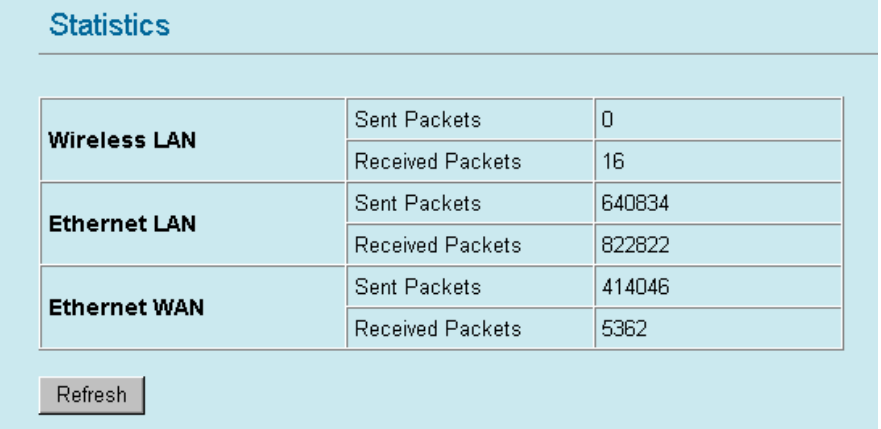
System



System	
Uptime	The time period since the device was up.
Firmware Version	The current version of the firmware installed in this device.
Wireless	
Mode	There are 7 modes supported, The default mode is **Access Point**. If you want to change to other mode, please click the Mode and select the wireless mode you want.
SSID	Display the SSID of this device

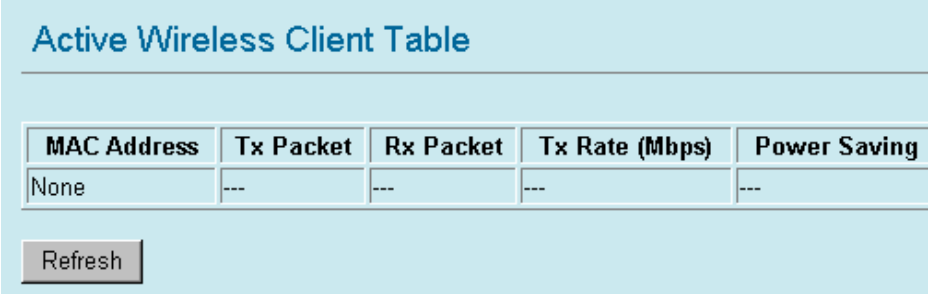
Channel Number	The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.
Encryption	WEP Encryption (Wired Equivalent Privacy) is set to **Disabled** by default. When WEP is enabled, data packet is encrypted before being transmitted. The WEP prevents data packets from being eavesdropped by unrelated people. By using WEP data encryption, there may be a significant degradation of the data throughput on the wireless link.
Associated Clients	Displays the total number of clients associated to this AP. You can have up to 64 clients to associate to this Access Point.
BSSID	**BSSID** displays the ID of current BSS, which uniquely identifies each BSS. In AP mode, this value is the MAC address of this Access Point.
LAN Configuration (TCP/IP)	
Connection Method:	Display the connection method, you can setup in TCP/IP section
Physical Address:	Display the LAN MAC address
IP Address:	Display the LAN IP address, you can setup in TCP/IP section
Network Mask:	Display the network mask, you can setup in TCP/IP section
Default Gateway:	Display the default gateway ip , you can setup in TCP/IP section
DHCP Server:	Default the DHCP Server is enabled(ON)
DHCP Start IP Address:	Display the DHCP server start IP address.
DHCP Finish IP Address:	Display the DHCP server finish IP address.
Internet Configuration	
Connection Method:	Display the internet connection method, you can setup in WISP mode→WAN Port configuration
Physical Address:	Display the AP MAC address.information
IP Address:	Display the internet IP Address, you can setup in WISP mode→WAN Port configuration
Network Mask:	Display the network mask, you can setup in WISP mode→WAN Port configuration
Default Gateway:	Display the default gateway , you can setup in WISP mode→WAN Port configuration

Statistics



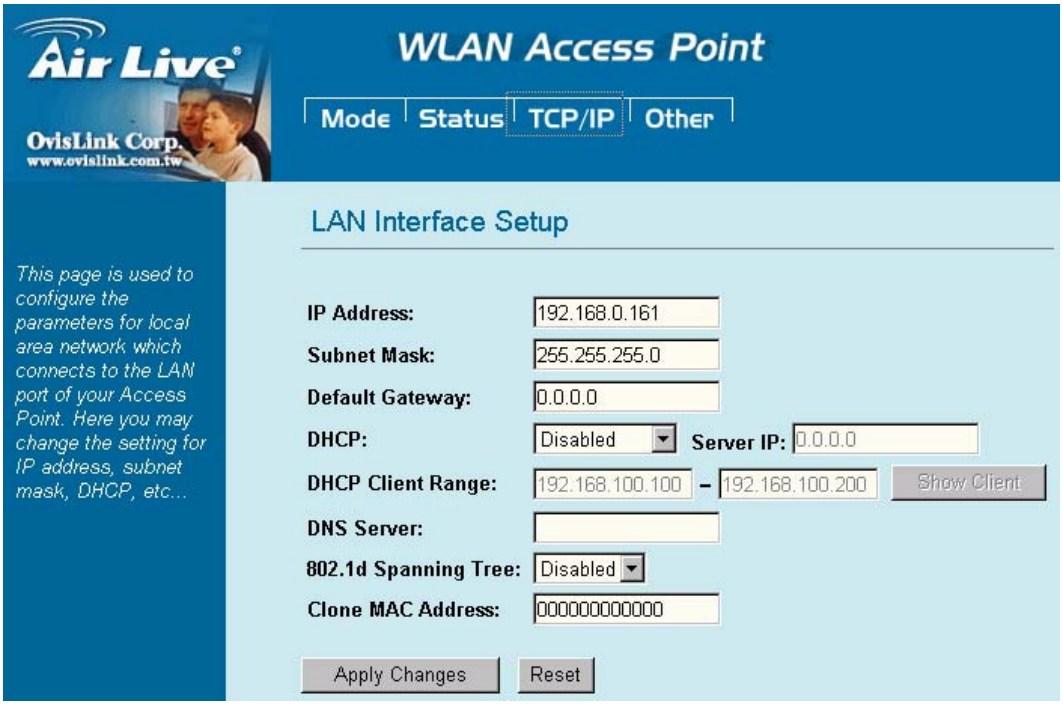
The Statistics table shows the packets sent/received over wireless and ethernet LAN respectively

Active Clients



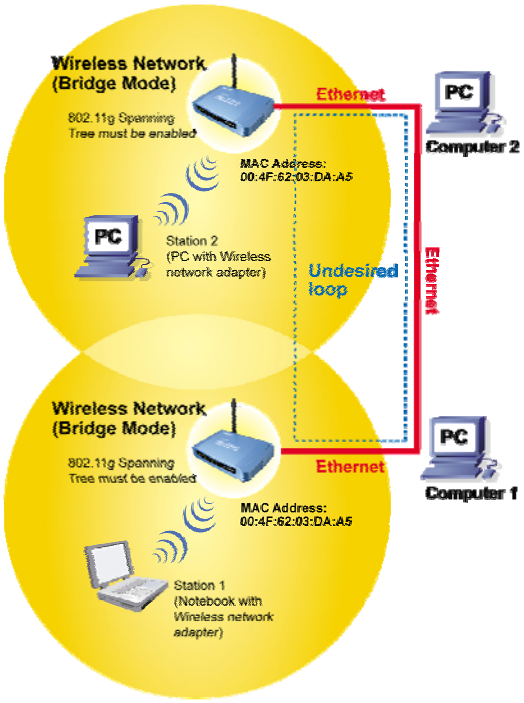
Display the active Wireless Clients table, and show wierless MAC address, TX/Rx Packet information

TCP / IP

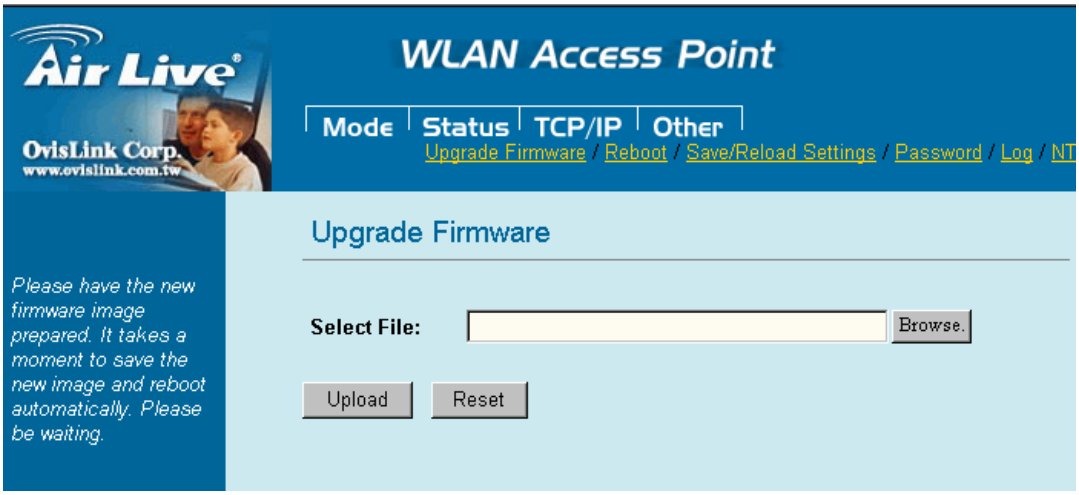


In this page, you can change the TCP/IP settings of this Access Point, select to enable/disable the DHCP Client, 802.1d Spanning Tree, and Clone MAC Address.

IP Address	This field can be modified only when DHCP Client is disabled. If your system manager assigned you static IP settings, then you will have to enter the information provided.
Subnet Mask	Enter the information provided by your system manager.
Default Gateway	Enter the information provided by your system manager.
DHCP	Select **Disable**, **Client** or **Server** from the pull-down menu. **Disable:** Select to disable DHCP server function. **Client:** Select to automatically get the LAN port IP address from ISP (For ADSL/Cable Modem). **Server:** Select to enable DHCP server function.
DHCP Client Range	WL-5060AP IP addresses continuing from 192.168.100.1 to 192.168.100.253
Show Client	Click to show Active DHCP Client table.
DNS Server	Enter the Domain Name Service IP address.
802.1d Spanning Tree	To enable 802.1d Spanning Tree will prevent the network from infinite loops. Infinite loop will happen in the network when WDS is enabled and there are multiple active paths between stations.–

	
Clone MAC Address	You can specify the MAC address of your Access Point to replace the factory setting.
Apply Change	Press to save the new settings on the screen.
Reset	Press to discard the data you have entered since last time you press Apply Change.

Upgrade Firmware

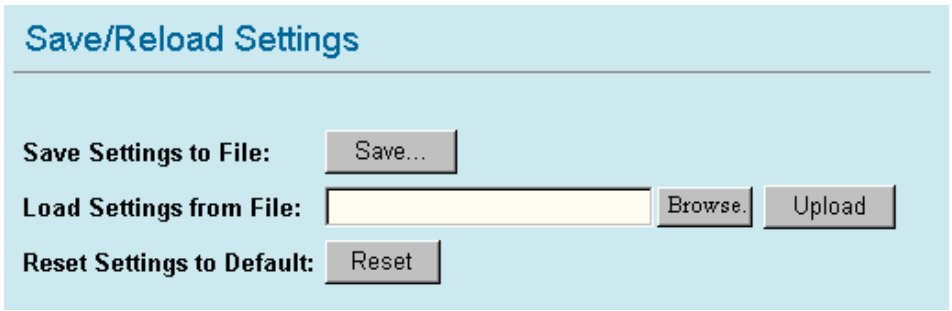


1. Download the latest firmware from your distributor and save the file on the hard drive.
2. Start the browser, open the configuration page, click on **Other,** and click **Upgrade Firmware** to enter the **Upgrade Firmware** window. Enter the new firmware's path and file name (i.e. C:\FIRMWARE\firmware.bin). Or, click the **Browse** button, find and open the firmware file (the browser will display to correct file path).
3. Click **Reset** to clear all the settings on this page. Or click **Upload** to start the upgrade.

Reboot

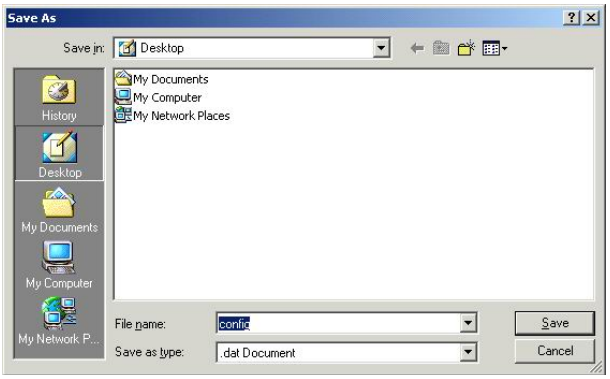
Click the reboot button to reboot this device.

Save / Reload Settings



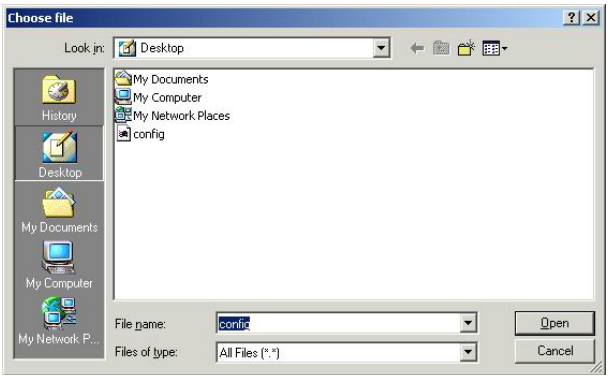
This function enables users to save the current configurations as a file (i.e. **config.dat**) To load configuration from a file, enter the file name or click **Browse...** to find the file from your computer.

Save Settings to File: Click **SAVE..** to save the current configuration to file.



When prompted the upper left screen, select "**Save this file to disk**", and the upper right screen will prompt you a dialog box to enter the file name and the file location.

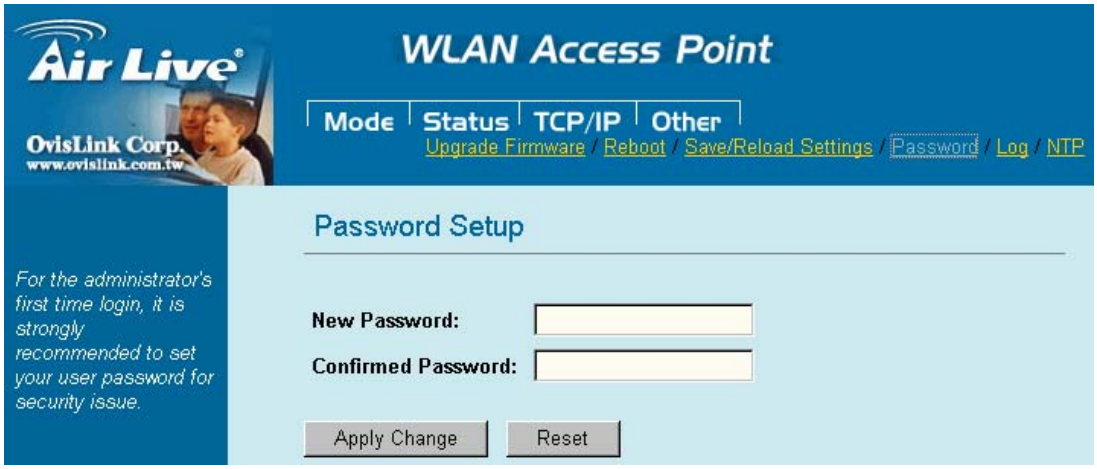
Load Settings From File: Click **Browse...** if you want to load a pre-saved file, enter the file name with the correct path and then click on **Upload**. Or click **Browse...** to select the file.



Reset: Click to restore the default configuration.

Password

For secure reason, it is recommended that you set the account to access the web server of this Access Point. Leaving the password blank will disable the protection. The login screen prompts immediately once you finish setting assword. Remember your password for you will be asked to enter them every time you access the web server of this Access Point.



New Password	Set your new password. Password can be up to 30 characters long. Password can contain letter, number and space. It is case sensitive.
Confirm Password	Re-enter the new password for confirmation.
Apply Change	Press to save the new settings on the screen.
Reset	Press to discard the data you have entered since last time you press Apply Change.

Note: when you setup the password and click the apply change button, system will pop-up Window and ask the username and password, please enter system default username "**admin**" (**not changeable**) and your password for entering the configuration WEB UI.